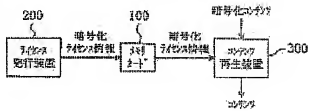
EQUIPMENT FOR ISSUING LICENSE, EQUIPMENT FOR REPRODUCING CONTENTS, METHOD FOR ISSUING LICENSE AND METHOD FOR REPRODUCING CONTENTS

Publication number: JP2002073421 (A)
Publication date: 2002-03-12
Inventor(s): AKASHI TERUO +
Applicant(s): MATSUSHITA ELECTRIC IND CO LTD +
Classification:
- international: ***G06F1/00; G06F12/14; G06F15/00; G06F21/00; G06F21/22; G06F21/24; G06Q30/00; G06Q50/00; H04L9/08; H04L9/32;*** **G06F1/00; G06F12/14; G06F15/00; G06F21/00; G06F21/22; G06Q30/00; G06Q50/00; H04L9/08; H04L9/32;** (IPC1-7): G06F1/00; G06F12/14; G06F15/00; G06F17/60; H04L9/08; H04L9/32
- European: G06F21/00N7D
Application number: JP20000262912 20000831
Priority number(s): JP20000262912 20000831

Also published as:
US2002026424 (A1)

Abstract of **JP 2002073421 (A)**
PROBLEM TO BE SOLVED: To provide an equipment and a method by which user can uses contents without being limited by an equipment of play back. SOLUTION: An equipment for issuing license 200 encodes license information about contents which user wants, using an equipment ID of memory card 100 which user carries, and writes it into the memory card. An equipment for reproducing contents 300 decodes license information that is written into the memory card 100 which user carries, using an equipment ID of the memory card 100. And an equipment for reproducing contents 300 decodes contents that is decoded according to contents that is permitted to use license information that is decoded and reproduce it.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－73421
（P2002－73421A）
(43)公開日　平成14年３月12日(2002.3.12)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｂ	５Ｂ０１７
			３２０Ｃ	５Ｂ０４９
1/00		15/00	３３０Ｚ	５Ｂ０７６
15/00	３３０	17/60	１４２	５Ｂ０８５
17/60	１４２		３０２Ｅ	５Ｊ１０４

審査請求　有　請求項の数19　ＯＬ　（全 18 頁）　最終頁に続く

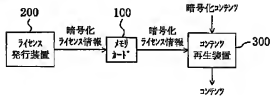
(21)出願番号　特願2000－262912(P2000－262912)
(22)出願日　平成12年８月31日(2000.8.31)

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　明石　輝夫
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(74)代理人　100077931
弁理士　前田　弘　（外７名）

Ｆターム(参考)　5B017 AA03 BA05 BA07 CA14 CA16
5B049 AA05 CC06 CG10
5B076 FA05 FB06 FB11
5B085 AE13 AE23 AE29
5J104 AA07 AA12 AA16 EA03 KA02
NA02 NA05 NA36 NA38 NA41

(54)【発明の名称】　ライセンス発行装置、コンテンツ再生装置、ライセンス発行方法、およびコンテンツ再生方法

(57)【要約】
【課題】　再生装置に限定されずにコンテンツを利用できるようにする。
【解決手段】　ライセンス発行装置２００は、利用者が希望するコンテンツのライセンス情報を、利用者が携帯するメモリカード１００の装置ＩＤを用いて暗号化して、当該メモリカード１００に書き込む。コンテンツ再生装置３００は、利用者が携帯するメモリカード１００に書き込まれたライセンス情報を、当該メモリカード１００の装置ＩＤを用いて復号する。そして、コンテンツ再生装置３００は、復号したライセンス情報において利用を許可されているコンテンツに対応する暗号化コンテンツを復号して再生する。



【特許請求の範囲】
【請求項１】　自己を一意に識別することができる装置ＩＤと相手装置の正当性を認証する機能とを有する携帯可能なライセンス記憶装置に、コンテンツの利用を許可するライセンス情報を書き込むライセンス発行装置であって、
利用者が携帯するライセンス記憶装置の正当性を認証する認証手段と、
前記利用者が携帯するライセンス記憶装置が正当なものであると前記認証手段によって認証されたとき、前記利用者によって指定されたコンテンツの利用を許可するライセンス情報を作成する手段と、
前記ライセンス情報作成手段によって作成されたライセンス情報を前記利用者が携帯するライセンス記憶装置の装置ＩＤを用いて暗号化して、当該暗号化したライセンス情報を前記利用者が携帯するライセンス記憶装置に書き込む第１の暗号化手段とを備えることを特徴とするライセンス発行装置。
【請求項２】　請求項１に記載のライセンス発行装置において、
前記ライセンス情報は、
前記利用者によって指定されたコンテンツを識別するためのコンテンツＩＤを含むことを特徴とするライセンス発行装置。
【請求項３】　請求項１に記載のライセンス発行装置において、
前記ライセンス情報は、
前記利用者によって指定されたコンテンツを利用する際の制限事項を示すコンテンツ利用条件を含むことを特徴とするライセンス発行装置。
【請求項４】　請求項１に記載のライセンス発行装置において、
前記ライセンス情報は、
前記利用者によって指定されたコンテンツを復号するための復号化鍵を含むことを特徴とするライセンス発行装置。
【請求項５】　請求項１に記載のライセンス発行装置において、
前記認証手段は、
前記利用者が携帯するライセンス記憶装置が有する装置鍵を用いて、前記利用者が携帯するライセンス記憶装置の装置ＩＤを暗号化する第２の暗号化手段を含み、
前記第１の暗号化手段は、
前記第２の暗号化手段によって暗号化された装置ＩＤを用いて前記ライセンス情報を暗号化して、当該暗号化したライセンス情報を前記利用者が携帯するライセンス記憶装置に書き込むことを特徴とするライセンス発行装置。
【請求項６】　請求項１に記載のライセンス発行装置において、
前記ライセンス発行装置は、前記利用者が携帯するライセンス記憶装置にネットワークを介して接続されることを特徴とするライセンス発行装置。
【請求項７】　暗号化されたコンテンツを復号して再生するコンテンツ再生装置であって、
前記コンテンツ再生装置は、
自己を一意に識別することができる装置ＩＤと相手装置の正当性を認証する機能とを有する携帯可能なライセンス記憶装置の装置ＩＤを用いて暗号化されて当該ライセンス記憶装置に記憶されたライセンス情報に基づいてコンテンツを復号して再生するものであり、
利用者が携帯するライセンス記憶装置の正当性を認証する認証手段と、
前記利用者が携帯するライセンス記憶装置が正当なものであると前記認証手段によって認証されたとき、前記利用者が携帯するライセンス記憶装置に記憶されたライセンス情報を、当該ライセンス記憶装置の装置ＩＤを用いて復号する復号手段と、
前記復号手段によって得られたライセンス情報において利用を許可されているコンテンツに対応する暗号化されたコンテンツを復号して再生する再生手段とを備えることを特徴とするコンテンツ再生装置。
【請求項８】　請求項７に記載のコンテンツ再生装置において、
前記利用者が携帯するライセンス記憶装置に記憶されたライセンス情報は、当該ライセンス情報において利用を許可されているコンテンツを復号するための復号化鍵を含むものであり、
前記再生手段は、
前記復号手段によって得られたライセンス情報に含まれる復号化鍵を用いて、当該ライセンス情報おいて利用を許可されているコンテンツに対応する暗号化されたコンテンツを復号することを特徴とするコンテンツ再生装置。
【請求項９】　請求項７に記載のコンテンツ再生装置において、
前記利用者が携帯するライセンス記憶装置に記憶されたライセンス情報は、当該ライセンス情報において利用を許可されているコンテンツを識別するためのコンテンツＩＤを含むものであり、
前記再生手段は、
前記復号手段によって得られたライセンス情報に含まれるコンテンツＩＤを用いて、当該ライセンス情報おいて利用を許可されているコンテンツに対応する暗号化されたコンテンツを取得することを特徴とするコンテンツ再生装置。
【請求項１０】　請求項７に記載のコンテンツ再生装置において、
前記コンテンツ再生装置はさらに、
暗号化されたコンテンツを蓄積する手段を備え、

前記再生手段は、
前記復号手段によって得られたライセンス情報において利用を許可されているコンテンツに対応する暗号化されたコンテンツを前記蓄積手段から取得することを特徴とするコンテンツ再生装置。
【請求項１１】　請求項７に記載のコンテンツ再生装置において、
前記再生手段は、
前記復号手段によって得られたライセンス情報において利用を許可されているコンテンツに対応する暗号化されたコンテンツをネットワークを介して取得することを特徴とするコンテンツ再生装置。
【請求項１２】　請求項７に記載のコンテンツ再生装置において、
前記利用者が携帯するライセンス記憶装置に記憶されたライセンス情報は、当該ライセンス情報において利用を許可されているコンテンツを利用する際の制限事項を示すコンテンツ利用条件を含むものであり、
前記再生手段は、
前記復号手段によって得られたライセンス情報に含まれるコンテンツ利用条件に従って、当該ライセンス情報において利用を許可されているコンテンツに対応する暗号化されたコンテンツを復号して再生することを特徴とするコンテンツ再生装置。
【請求項１３】　請求項１２に記載のコンテンツ再生装置において、
前記コンテンツ再生装置はさらに、
前記復号手段によって得られたライセンス情報に含まれるコンテンツ利用条件を、前記再生手段によるコンテンツの再生に応じて更新するコンテンツ利用条件更新手段と、
前記復号手段によって得られたライセンス情報に含まれるコンテンツ利用条件に代えて前記コンテンツ利用条件更新手段によって更新されたコンテンツ利用条件を含んだ更新後ライセンス情報を生成する手段と、
前記更新後ライセンス情報生成手段によって生成された更新後ライセンス情報を前記利用者が携帯するライセンス記憶装置の装置ＩＤを用いて暗号化する手段と、
前記利用者が携帯するライセンス記憶装置に記憶されたライセンス情報を、前記暗号化手段によって暗号化された更新後ライセンス情報に書き換える手段とを備えることを特徴とするコンテンツ再生装置。
【請求項１４】　暗号化されたコンテンツを復号して再生するコンテンツ再生装置であって、
前記コンテンツ再生装置は、
自己を一意に識別することができる装置ＩＤと相手装置の正当性を認証する機能とを有する携帯可能なライセンス記憶装置の装置鍵を用いて暗号化された当該ライセンス記憶装置の装置ＩＤ、を用いて暗号化されて当該ライセンス記憶装置に記憶されたライセンス情報に基づいてコンテンツを復号して再生するものであり、
利用者が携帯するライセンス記憶装置の正当性を認証し、当該ライセンス記憶装置が正当であると認証されたとき、当該ライセンス記憶装置の装置鍵を用いて当該ライセンス記憶装置の装置ＩＤを暗号化して暗号化装置ＩＤを生成する認証手段と、
前記利用者が携帯するライセンス記憶装置に記憶されたライセンス情報を、前記認証手段によって生成された暗号化装置ＩＤを用いて復号する復号手段と、
前記復号手段によって得られたライセンス情報において利用を許可されているコンテンツに対応する暗号化されたコンテンツを復号して再生する再生手段とを備えることを特徴とするコンテンツ再生装置。
【請求項１５】　自己を一意に識別することができる装置ＩＤと相手装置の正当性を認証する機能とを有する携帯可能なライセンス記憶装置に、コンテンツの利用を許可するライセンス情報を書き込むライセンス発行方法であって、
利用者が携帯するライセンス記憶装置の正当性を認証し、
前記利用者が携帯するライセンス記憶装置が正当なものであると認証されたとき、
前記利用者によって指定されたコンテンツの利用を許可するライセンス情報を前記利用者が携帯するライセンス記憶装置の装置ＩＤを用いて暗号化して、当該暗号化したライセンス情報を前記利用者が携帯するライセンス記憶装置に書き込むことを特徴とするライセンス発行方法。
【請求項１６】　暗号化されたコンテンツを復号して再生するコンテンツ再生方法であって、
前記コンテンツ再生方法は、
自己を一意に識別することができる装置ＩＤと相手装置の正当性を認証する機能とを有する携帯可能なライセンス記憶装置の装置ＩＤを用いて暗号化されて当該ライセンス記憶装置に記憶されたライセンス情報に基づいてコンテンツを復号して再生するものであり、
利用者が携帯するライセンス記憶装置の正当性を認証するステップと、
前記認証ステップにおいて前記利用者が携帯するライセンス記憶装置が正当なものであると認証されたとき、前記利用者が携帯するライセンス記憶装置に記憶されたライセンス情報を、当該ライセンス記憶装置の装置ＩＤを用いて復号するステップと、
前記復号ステップによって得られたライセンス情報において利用を許可されているコンテンツに対応する暗号化されたコンテンツを復号して再生するステップとを備えることを特徴とするコンテンツ再生方法。
【請求項１７】　請求項１６に記載のコンテンツ再生方法において、
前記再生ステップでは、

前記復号ステップによって得られたライセンス情報において利用を許可されているコンテンツに対応する暗号化されたコンテンツをネットワークを介して取得することを特徴とするコンテンツ再生方法。

【請求項18】 請求項16に記載のコンテンツ再生方法において、

前記利用者が携帯するライセンス記憶装置に記憶されたライセンス情報は、当該ライセンス情報において利用を許可されているコンテンツを利用する際の制限事項を示すコンテンツ利用条件を含むものであり、

前記再生ステップでは、

前記復号ステップによって得られたライセンス情報に含まれるコンテンツ利用条件に従って、当該ライセンス情報において利用を許可されているコンテンツに対応する暗号化されたコンテンツを復号して再生することを特徴とするコンテンツ再生方法。

【請求項19】 請求項18に記載のコンテンツ再生方法において、

前記復号ステップによって得られたライセンス情報に含まれるコンテンツ利用条件を、前記再生ステップにおけるコンテンツの再生に応じて更新するステップと、

前記復号ステップによって得られたライセンス情報に含まれるコンテンツ利用条件に代えて前記更新ステップによって更新されたコンテンツ利用条件を含んだ更新後ライセンス情報を、前記利用者が携帯するライセンス記憶装置の装置IDを用いて暗号化するステップと、

前記利用者が携帯するライセンス記憶装置に記憶されたライセンス情報を、前記暗号化ステップによって暗号化された更新後ライセンス情報に書き換えるステップとをさらに備えることを特徴とするコンテンツ再生方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、ライセンス発行装置、コンテンツ再生装置、ライセンス発行方法、およびコンテンツ再生方法に関する。さらに詳しくは、コンテンツと当該コンテンツのライセンスとを分離して提供するコンテンツ提供システムにおけるライセンス発行装置、コンテンツ再生装置、ライセンス発行方法、およびコンテンツ再生方法に関する。

【0002】

【従来の技術】デジタル技術の発達により、ソフトウエアプログラムのみならず、絵画、音楽、映画などの著作物もデジタルデータとして管理され、流通するようになっている。近年ではさらに、ネットワーク技術の著しい進歩により、これらの著作物を、時間と場所を問わず、ネットワークを介して利用者に配布することが可能な環境が整いつつある。

【0003】デジタルデータとしてのこれらのコンテンツは、従来のアナログデータと異なり、複製を繰り返しても品質が劣化しない。したがって、コンテンツを販売する側としては、流通しているコンテンツが著作権者の許可なく複製されるような不正利用を防止することが不可欠である。この点に関しては、暗号技術の発展がコンテンツのセキュリティレベルの向上に寄与している。暗号化技術としては、暗号化鍵と復号化鍵に同一の鍵を用いる対称暗号の一種であるDES や、暗号化と復号化で鍵の異なる非対称暗号のRSA暗号などが知られている。

【0004】コンテンツの不正利用を防ぐ技術の第1の例として、販売しようとするコンテンツの全部またはは一部をあらかじめ暗号化してそのままでは利用不可能な状態に保護しておき、利用者が保護状態を解除するためのライセンスを購入する、という販売方式がある。この方式では、コンテンツを再生する装置に固有のIDを認識し、配布するライセンスをこのIDを含めて暗号化しておく。そして、再生時に、ライセンスを復号化して取り出したIDと再生装置に固有のIDとを比較して一致した場合にのみ再生を行う。このように、コンテンツを再生できる装置を限定し、不正に複製された装置上での利用を防いでいる。

【0005】また、第2の例として、ネットワーク上に管理センターを設け、コンテンツの再生時に、ネットワークを介して管理センターに接続し、パスワード等によりあらかじめ登録された利用者の認証を行うという手法がある。

【0006】

【発明が解決しようとする課題】上述の第1の例においては、コンテンツをライセンスとともに購入した後では、コンテンツを再生できる装置はライセンスを受けた再生装置に限定される。このため、コンテンツが自由に流通するようになっても、そのコンテンツを利用するときには再生装置の制約を受ける。すなわち、特定のコンピュータにライセンスされたプログラムは、そのコンピュータにアクセスしなければ利用できない。家庭の据置型プレーヤにライセンスされた音楽は、外出先の携帯端末では利用できない。携帯型ビデオ再生装置にライセンスされた映画は、家庭内の大画面ディスプレイを備える装置では再生できない。このような種々の不具合が生じる。

【0007】また、上述の第2の例においては、ネットワークに接続でき、かつ管理センターと通信するための手段が不可欠となる。したがって、このような機能を持たない再生装置での利用は制限される。

【0008】

【課題を解決するための手段】この発明の1つの局面に従うと、ライセンス発行装置は、携帯可能なライセンス記憶装置に、コンテンツの利用を許可するライセンス情報を書き込むものである。ライセンス記憶装置は、自己を一意に識別することができる装置IDと相手装置の正当性を認証する機能とを有する。ライセンス発行装置

は、認証手段と、ライセンス情報作成手段と、第１の暗号化手段とを備える。認証手段は、利用者が携帯するライセンス記憶装置の正当性を認証する。ライセンス情報作成手段は、利用者が携帯するライセンス記憶装置が正当なものであると認証手段によって認証されたとき、利用者によって指定されたコンテンツの利用を許可するライセンス情報を作成する。第１の暗号化手段は、ライセンス情報作成手段によって作成されたライセンス情報を利用者が携帯するライセンス記憶装置の装置ＩＤを用いて暗号化して、当該暗号化したライセンス情報を利用者が携帯するライセンス記憶装置に書き込む。

【０００９】上記ライセンス発行装置では、利用者が希望するコンテンツのライセンス情報を、携帯可能な独立したハードウエアであるライセンス記憶装置に書き込む。したがって、利用者は、希望するコンテンツのライセンス情報が書き込まれたライセンス記憶装置を携帯し、ライセンス記憶装置に対応したさまざまな形態のコンテンツ再生装置を利用してコンテンツの提供を受けることができる。

【００１０】また、ライセンス情報は、ライセンス記憶装置の装置ＩＤを用いて暗号化される。これにより、暗号化ライセンス情報を不正にコピーしたライセンス記憶装置を用いてコンテンツの提供を受けるような不正な利用を防ぐことができる。

【００１１】また、上記ライセンス発行装置は、コンテンツのライセンス情報だけを利用者の携帯するライセンス記憶装置に書き込む。したがって、利用者が希望するコンテンツが大容量のコンテンツであっても、ライセンス情報の発行にかかる時間を増大させることがなく、また、利用者はライセンス記憶装置の記憶容量を気にする必要もない。

【００１２】また、ライセンス情報のデータ量はコンテンツのデータ量に比べて小さいため、利用者は１つのライセンス記憶装置でたくさんのコンテンツを利用することができる。

【００１３】好ましくは、上記ライセンス情報は、利用者によって指定されたコンテンツを識別するためのコンテンツＩＤを含む。

【００１４】好ましくは、上記ライセンス情報は、利用者によって指定されたコンテンツを利用する際の制限事項を示すコンテンツ利用条件を含む。

【００１５】好ましくは、上記ライセンス情報は、利用者によって指定されたコンテンツを復号するための復号化鍵を含む。

【００１６】好ましくは、上記認証手段は、第２の暗号化手段を含む。第２の暗号化手段は、利用者が携帯するライセンス記憶装置が有する装置鍵を用いて、利用者が携帯するライセンス記憶装置の装置ＩＤを暗号化する。そして、上記第１の暗号化手段は、第２の暗号化手段によって暗号化された装置ＩＤを用いてライセンス情報を暗号化して、当該暗号化したライセンス情報を利用者が携帯するライセンス記憶装置に書き込む。

【００１７】好ましくは、上記ライセンス発行装置は、利用者が携帯するライセンス記憶装置にネットワークを介して接続される。

【００１８】上記ライセンス発行装置によれば、利用者は、ライセンス発行装置と距離的に離れた所にいても、ネットワークを介してライセンス発行装置にアクセス可能な携帯端末などを用いて、ライセンス情報の発行を受けることができる。

【００１９】この発明のもう１つの局面に従うと、コンテンツ再生装置は、暗号化されたコンテンツを復号して再生するものである。また、コンテンツ再生装置は、携帯可能なライセンス記憶装置の装置ＩＤを用いて暗号化されて当該ライセンス記憶装置に記憶されたライセンス情報に基づいてコンテンツを復号して再生するものである。ライセンス記憶装置は、自己を一意に識別することができる装置ＩＤと相手装置の正当性を認証する機能とを有する。そして、コンテンツ再生装置は、認証手段と、復号手段と、再生手段とを備える。認証手段は、利用者が携帯するライセンス記憶装置の正当性を認証する。復号手段は、利用者が携帯するライセンス記憶装置が正当なものであると認証手段によって認証されたとき、利用者が携帯するライセンス記憶装置に記憶されたライセンス情報を、当該ライセンス記憶装置の装置ＩＤを用いて復号する。再生手段は、復号手段によって得られたライセンス情報において利用を許可されているコンテンツに対応する暗号化されたコンテンツを復号して再生する。

【００２０】上記コンテンツ再生装置では、利用者が携帯するライセンス記憶装置に書き込まれたライセンス情報を用いて暗号化コンテンツを復号し再生する。したがって、利用者は、希望するコンテンツのライセンス情報が書き込まれたライセンス記憶装置を携帯し、ライセンス記憶装置に対応したさまざまな形態のコンテンツ再生装置を利用してコンテンツの提供を受けることができる。

【００２１】また、利用者が携帯するライセンス記憶装置に書き込まれたライセンス情報は、当該ライセンス記憶装置の装置ＩＤを用いて復号される。これにより、暗号化ライセンス情報を不正にコピーしたライセンス記憶装置を用いてコンテンツの提供を受けるような不正な利用を防ぐことができる。

【００２２】好ましくは、上記利用者が携帯するライセンス記憶装置に記憶されたライセンス情報は、当該ライセンス情報において利用を許可されているコンテンツを復号するための復号化鍵を含む。そして、上記再生手段は、復号手段によって得られたライセンス情報に含まれる復号化鍵を用いて、当該ライセンス情報おいて利用を許可されているコンテンツに対応する暗号化されたコン

テンツを復号する。

【0023】好ましくは、上記利用者が携帯するライセンス記憶装置に記憶されたライセンス情報は、当該ライセンス情報において利用を許可されているコンテンツを識別するためのコンテンツＩＤを含む。そして、上記再生手段は、復号手段によって得られたライセンス情報に含まれるコンテンツＩＤを用いて、当該ライセンス情報おいて利用を許可されているコンテンツに対応する暗号化されたコンテンツを取得する。

【0024】好ましくは、上記コンテンツ再生装置はさらに、蓄積手段を備える。蓄積手段は、暗号化されたコンテンツを蓄積する。そして、上記再生手段は、復号手段によって得られたライセンス情報において利用を許可されているコンテンツに対応する暗号化されたコンテンツを蓄積手段から取得する。

【0025】上記コンテンツ再生装置では、再生する可能性のあるコンテンツをあらかじめすべて蓄積手段に蓄積しておくことにより、取得するのに時間のかかる大容量のコンテンツであっても即座に再生することができる。

【0026】好ましくは、上記再生手段は、復号手段によって得られたライセンス情報において利用を許可されているコンテンツに対応する暗号化されたコンテンツをネットワークを介して取得する。

【0027】上記コンテンツ再生装置では、コンテンツの再生時にその都度暗号化コンテンツをネットワークを介して取得する。これにより、仮想的に容量が無限大のコンテンツサーバを所有することと同様の効果が得られる。

【0028】好ましくは、上記利用者が携帯するライセンス記憶装置に記憶されたライセンス情報は、当該ライセンス情報において利用を許可されているコンテンツを利用する際の制限事項を示すコンテンツ利用条件を含む。そして、上記再生手段は、復号手段によって得られたライセンス情報に含まれるコンテンツ利用条件に従って、当該ライセンス情報において利用を許可されているコンテンツに対応する暗号化されたコンテンツを復号して再生する。

【0029】好ましくは、上記コンテンツ再生装置はさらに、コンテンツ利用条件更新手段と、更新後ライセンス情報生成手段と、暗号化手段と、書き換え手段とを備える。コンテンツ利用条件更新手段は、復号手段によって得られたライセンス情報に含まれるコンテンツ利用条件を、再生手段によるコンテンツの再生に応じて更新する。更新後ライセンス情報生成手段は、復号手段によって得られたライセンス情報に含まれるコンテンツ利用条件に代えてコンテンツ利用条件更新手段によって更新されたコンテンツ利用条件を含んだ更新後ライセンス情報を生成する。暗号化手段は、更新後ライセンス情報生成手段によって生成された更新後ライセンス情報を利用者が携帯するライセンス記憶装置の装置ＩＤを用いて暗号化する。書き換え手段は、利用者が携帯するライセンス記憶装置に記憶されたライセンス情報を、暗号化手段によって暗号化された更新後ライセンス情報に書き換える。

【0030】上記コンテンツ再生装置では、コンテンツの再生に応じてコンテンツ利用条件が変化する場合でも、コンテンツ利用条件を更新することができ、正しいコンテンツ利用条件を保持することができる。

【0031】この発明のさらにもう1つの局面に従うと、コンテンツ再生装置は、暗号化されたコンテンツを復号して再生するものである。また、コンテンツ再生装置は、携帯可能なライセンス記憶装置の装置鍵を用いて暗号化された当該ライセンス記憶装置の装置ＩＤ、を用いて暗号化されて当該ライセンス記憶装置に記憶されたライセンス情報に基づいてコンテンツを復号して再生するものである。ライセンス記憶装置は、自己を一意に識別することができる装置ＩＤと相手装置の正当性を認証する機能とを有する。そして、コンテンツ再生装置は、認証手段と、復号手段と、再生手段とを備える。認証手段は、利用者が携帯するライセンス記憶装置の正当性を認証し、当該ライセンス記憶装置が正当であると認証されたとき、当該ライセンス記憶装置の装置鍵を用いて当該ライセンス記憶装置の装置ＩＤを暗号化して暗号化装置ＩＤを生成する。復号手段は、利用者が携帯するライセンス記憶装置に記憶されたライセンス情報を、認証手段によって生成された暗号化装置ＩＤを用いて復号する。再生手段は、復号手段によって得られたライセンス情報において利用を許可されているコンテンツに対応する暗号化されたコンテンツを復号して再生する。

【0032】この発明のさらにもう1つの局面に従うと、ライセンス発行方法は、携帯可能なライセンス記憶装置に、コンテンツの利用を許可するライセンス情報を書き込むものである。ライセンス記憶装置は、自己を一意に識別することができる装置ＩＤと相手装置の正当性を認証する機能とを有する。そして、ライセンス発行方法は、認証ステップと、書き込みステップとを備える。認証ステップでは、利用者が携帯するライセンス記憶装置の正当性を認証する。書き込みステップでは、利用者が携帯するライセンス記憶装置が正当なものであると認証ステップによって認証されたとき、利用者によって指定されたコンテンツの利用を許可するライセンス情報を利用者が携帯するライセンス記憶装置の装置ＩＤを用いて暗号化して、当該暗号化したライセンス情報を利用者が携帯するライセンス記憶装置に書き込む。

【0033】上記ライセンス発行方法では、利用者が希望するコンテンツのライセンス情報を、携帯可能な独立したハードウエアであるライセンス記憶装置に書き込む。したがって、利用者は、希望するコンテンツのライセンス情報が書き込まれたライセンス記憶装置を携帯

し、さまざまな形態のコンテンツ再生装置を利用してコンテンツの提供を受けることができる。

【0034】また、ライセンス情報は、ライセンス記憶装置の装置ＩＤを用いて暗号化される。これにより、暗号化ライセンス情報を不正にコピーしたライセンス記憶装置を用いてコンテンツの提供を受けるような不正な利用を防ぐことができる。

【0035】また、上記ライセンス発行方法では、コンテンツのライセンス情報だけを利用者の携帯するライセンス記憶装置に書き込む。したがって、利用者が希望するコンテンツが大容量のコンテンツであっても、ライセンス情報の発行にかかる時間を増大させることがなく、また、利用者はライセンス記憶装置の記憶容量を気にする必要もない。

【0036】また、ライセンス情報のデータ量はコンテンツのデータ量に比べて小さいため、利用者は１つのライセンス記憶装置でたくさんのコンテンツを利用することができる。

【0037】この発明のさらにもう１つの局面に従うと、コンテンツ再生方法は、暗号化されたコンテンツを復号して再生するものである。また、コンテンツ再生方法は、携帯可能なライセンス記憶装置の装置ＩＤを用いて暗号化されて当該ライセンス記憶装置に記憶されたライセンス情報に基づいてコンテンツを復号して再生するものである。ライセンス記憶装置は、自己を一意に識別することができる装置ＩＤと相手装置の正当性を認証する機能とを有する。そして、コンテンツ再生方法は、認証ステップと、復号ステップと、再生ステップとを備える。認証ステップでは、利用者が携帯するライセンス記憶装置の正当性を認証する。復号ステップでは、認証ステップにおいて利用者が携帯するライセンス記憶装置が正当なものであると認証されたとき、当該利用者が携帯するライセンス記憶装置に記憶されたライセンス情報を、当該ライセンス記憶装置の装置ＩＤを用いて復号する。再生ステップでは、復号ステップによって得られたライセンス情報において利用を許可されているコンテンツに対応する暗号化されたコンテンツを復号して再生する。

【0038】上記コンテンツ再生方法では、利用者が携帯するライセンス記憶装置に書き込まれたライセンス情報を用いて暗号化コンテンツを復号し再生する。したがって、利用者は、希望するコンテンツのライセンス情報が書き込まれたライセンス記憶装置を携帯し、さなざまな形態のコンテンツの提供を受けることができる。

【0039】また、利用者が携帯するライセンス記憶装置に書き込まれたライセンス情報は、当該ライセンス記憶装置の装置ＩＤを用いて復号される。これにより、暗号化ライセンス情報を不正にコピーしたライセンス記憶装置を用いてコンテンツの提供を受けるような不正な利用を防ぐことができる。

【0040】好ましくは、上記再生ステップでは、復号ステップによって得られたライセンス情報において利用を許可されているコンテンツに対応する暗号化されたコンテンツをネットワークを介して取得する。

【0041】上記コンテンツ再生方法では、コンテンツの再生時にその都度暗号化コンテンツをネットワークを介して取得する。これにより、仮想的に容量が無限大のコンテンツサーバを所有することと同様の効果が得られる。

【0042】好ましくは、上記利用者が携帯するライセンス記憶装置に記憶されたライセンス情報は、当該ライセンス情報において利用を許可されているコンテンツを利用する際の制限事項を示すコンテンツ利用条件を含むものである。そして、上記再生ステップでは、復号ステップによって得られたライセンス情報に含まれるコンテンツ利用条件に従って、当該ライセンス情報において利用を許可されているコンテンツに対応する暗号化されたコンテンツを復号して再生する。

【0043】好ましくは、上記コンテンツ再生方法はさらに、更新ステップと、暗号化ステップと、書き換えステップとを備える。更新ステップでは、復号ステップによって得られたライセンス情報に含まれるコンテンツ利用条件を、再生ステップにおけるコンテンツの再生に応じて更新する。暗号化ステップでは、復号ステップによって得られたライセンス情報に含まれるコンテンツ利用条件に代えて更新ステップによって更新されたコンテンツ利用条件を含んだ更新後ライセンス情報を、利用者が携帯するライセンス記憶装置の装置ＩＤを用いて暗号化する。書き換えステップでは、利用者が携帯するライセンス記憶装置に記憶されたライセンス情報を、暗号化ステップによって暗号化された更新後ライセンス情報に書き換える。

【0044】上記コンテンツ再生方法では、コンテンツの再生に応じてコンテンツ利用条件が変化する場合でも、コンテンツ利用条件を更新することができ、正しいコンテンツ利用条件を保持することができる。

【0045】

【発明の実施の形態】以下、この発明の実施の形態を図面を参照して詳しく説明する。なお、図中同一または相当部分には同一符号を付し、その説明は繰り返さない。また、この発明では暗号アルゴリズムに制限を設けていないが、以下の実施の形態における説明では、特に断りのない限り暗号アルゴリズムとして暗号鍵と復号鍵に同一の鍵を用いる共通鍵暗号方式を想定している。

【0046】（第１の実施形態）図１は、この発明の第１の実施形態によるコンテンツ提供システムの構成を示す図である。図１を参照して、このコンテンツ提供システムでは、ソフトウエア、音楽、映像などの電子的な著作物であるデジタルコンテンツ（以下、コンテンツという。）と、当該コンテンツの利用を許可するライセンス

情報とが分離して配布される。コンテンツは、そのままでは利用ができないように暗号化して暗号化コンテンツとして配布される。また、暗号化コンテンツは、ネットワーク、放送、パッケージなどさまざまな形態で配布される。

【0047】コンテンツの提供を希望する利用者は、メモリカード100をライセンス発行装置200に挿入する。ライセンス発行装置200は、利用者が希望するコンテンツの利用を許可するライセンス情報と、利用者が携帯するメモリカード100の装置IDを用いて暗号化して、当該メモリカード100に書き込む。すなわち、メモリカード100には暗号化ライセンス情報だけが書き込まれる。そして利用者は、暗号化ライセンス情報が書き込まれたメモリカード100をコンテンツ再生装置300に挿入する。コンテンツ再生装置300は、利用者が携帯するメモリカード100に書き込まれたライセンス情報を、当該メモリカード100の装置IDを用いて復号する。そして、コンテンツ再生装置300は、復号したライセンス情報において利用を許可されているコンテンツに対応する暗号化コンテンツを復号して再生する。このようにして、コンテンツと、当該コンテンツの利用を許可するライセンス情報とが提供される。

【0048】以下、図1に示したメモリカード100、ライセンス発行装置200、およびコンテンツ再生装置300の具体的な構成、ライセンス発行装置200によるライセンス情報の発行の手順、ならびにコンテンツ再生装置300によるコンテンツの再生の手順について詳しく説明する。

【0049】図2は、図1に示したメモリカード100およびライセンス発行装置200の具体的な構成を示すブロック図である。以下、図2を参照しつつ説明する。

【0050】<メモリカード100の構成>メモリカード100は、携帯可能な独立したハードウエアであり、自己を一意に識別可能な装置IDを有する。そして、メモリカード100は、装置ID読み出し手段110と、相手装置認証手段120と、ライセンス記憶手段130とを備える。

【0051】装置ID読み出し手段110は、メモリカード100が有する装置IDを読み出して出力する。

【0052】相手装置認証手段120は、ライセンス情報を送受信する相手装置が正当な装置かどうかを認証する。相手装置は、ライセンス発行装置200からライセンス情報の提供を受ける場合には発行装置200であり、コンテンツ再生装置300によってコンテンツの提供を受ける場合にはコンテンツ再生装置300である。相手装置認証手段120は、例えば、使用不可能なライセンス情報を発行してライセンス料のみを得るというような不正なライセンス発行装置を排除するために必要である。

【0053】ライセンス記憶手段130は、ライセンス発行装置200からの暗号化されたライセンス情報を記憶する。ライセンス記憶手段130としては、例えば、フラッシュメモリなどが挙げられる。

【0054】<ライセンス発行装置200の構成>ライセンス発行装置200は、メモリカード認証手段210と、コンテンツID入力手段220と、コンテンツ利用条件入力手段230と、コンテンツ復号化鍵取得手段240と、連結手段250と、暗号化手段260とを備える。

【0055】メモリカード認証手段210は、メモリカード100が正当なものであるかどうかを認証する。メモリカード認証手段210は、認証に先立ってメモリカード100から装置IDを取得する。そしてメモリカード100との間で相互に認証を行った後、装置IDを暗号化して暗号化装置IDを出力する。これは、コンテンツを再生する際にコンテンツ再生装置300で同一の鍵を得るためである。

【0056】コンテンツID入力手段220は、利用者が指定したコンテンツに対するコンテンツIDを出力する。コンテンツIDとは、各コンテンツを識別するための記号である。コンテンツID入力手段220としては、例えば、キーボードやタッチパネルなどの入力装置によって利用者に直接に所望のコンテンツに対応したコンテンツIDの入力を促し、入力されたコンテンツIDをそのまま出力するものが挙げられる。また、別の例としては、ライセンス情報の発行が可能なコンテンツタイトルの一覧をディスプレイなどに表示して利用者に選択を促し、選択されたコンテンツタイトルに対するコンテンツID を、図3に示すようなコンテンツタイトル31とコンテンツID32とが対応づけられたデータベースから取得するというものが挙げられる。なお、図3に示すデータベースでは、コンテンツタイトル31、コンテンツID32、およびコンテンツ復号化鍵33の対応づけられている。そして、コンテンツ復号化鍵33の情報は、外部から読み出すことができないように保護されている。

【0057】コンテンツ利用条件入力手段230は、コンテンツ利用条件を出力する。コンテンツ利用条件とは、コンテンツを利用する際の制限事項を示す情報である。コンテンツ利用条件としては、例えば、コンテンツがソフトウエアプログラムである場合に、「扱うデータ量は100Kバイトまでとする」というような制限事項を示す情報が挙げられる。また、別の例としては、コンテンツが音楽データの場合に、「再生することができる期間」を示す情報が挙げられる。コンテンツ利用条件はコンテンツの特性に応じてさまざまなものが考えられるため、コンテンツまたはコンテンツのカテゴリに対応した利用条件データベースを設けてもよい。この場合にも、上述したコンテンツID入力手段220におけるのと同様に、利用者に利用条件の一覧を提示して利用者に

選択を促すなどの方法がある。

【００５８】コンテンツ復号化鍵取得手段２４０は、コンテンツＩＤ入力手段２２０からのコンテンツＩＤを受け、当該コンテンツＩＤに対応するコンテンツを暗号化された状態から復号するための鍵を取得する。例えば、図３に示したデータベースを参照して取得することができる。

【００５９】連結手段２５０は、コンテンツＩＤ入力手段２２０からのコンテンツＩＤ、コンテンツ利用条件入力手段２３０からのコンテンツ利用条件、およびコンテンツ復号化鍵取得手段２４０からのコンテンツ復号化鍵を連結してライセンス情報を生成する。

【００６０】暗号化手段２６０は、連結手段２５０によって生成されたライセンス情報をメモリカード認証手段２１０からの暗号化装置ＩＤで暗号化して暗号化ライセンス情報を生成する。そして、暗号化手段２６０は、暗号化ライセンス情報をメモリカード１００のライセンス記憶手段１３０へ書き込む。

【００６１】<ライセンス情報の発行の手順>図４は、図２に示したライセンス発行装置２００によるライセンス情報の発行の手順を示すフローチャートである。以下、図４および図２を参照しつつライセンス情報の発行の手順について説明する。

【００６２】まず、ステップＳＴ４０１において、利用者は、メモリカード１００をライセンス発行装置２００の所定の挿入口に差し込む。これにより、メモリカード１００に設けられたピンとライセンス発行装置２００のソケットとの間が電気的に接続される。この結果、メモリカード１００とライセンス発行装置２００との間で、お互いにデータを送受信するための通信手段が確保される。

【００６３】次いで、ステップＳＴ４０２において、メモリカード１００とライセンス発行装置２００との間で、お互いが正当な装置であることの認証が行われる。この相互認証の手順については後述する。相互認証中にエラーが発生した場合には処理が中断されて利用者にその旨が知らされる。相互認証を行った後、メモリカード認証手段２１０は、メモリカード１００の装置ＩＤを暗号化して暗号化装置ＩＤを生成する。

【００６４】次いで、ステップＳＴ４０３において、利用者は、コンテンツＩＤ入力手段２２０を利用して、希望するコンテンツに対応するコンテンツＩＤを入力する。これにより、利用者が希望するコンテンツに対応するコンテンツＩＤが得られる。

【００６５】次いで、ステップＳＴ４０４において、利用者は、コンテンツ利用条件入力手段２３０を利用して、コンテンツ利用条件を入力する。これにより、利用者が希望するコンテンツに対するコンテンツ利用条件が得られる。

【００６６】次いで、ステップＳＴ４０５において、利用者は、希望するコンテンツおよびその利用条件に対応した料金を支払う。料金の支払い手段／方法としては、種々の公知の手段／方法を利用することができる。

【００６７】次いで、ステップＳＴ４０６において、コンテンツ復号化鍵取得手段２４０は、ステップＳＴ４０３において得られたコンテンツＩＤに対応するコンテンツを暗号化された状態から復号するための鍵を取得する。ここでは、図３に示したデータベースを参照して取得する。

【００６８】次いで、ステップＳＴ４０７において、連結手段２５０は、ステップＳＴ４０３において得られたコンテンツＩＤ、ステップＳＴ４０４において得られたコンテンツ利用条件、およびステップＳＴ４０６において得られたコンテンツ復号化鍵を連結してライセンス情報を生成する。

【００６９】次いで、ステップＳＴ４０８において、暗号化手段２６０は、ステップＳＴ４０７において得られたライセンス情報をステップＳＴ４０２において得られた暗号化装置ＩＤで暗号化して暗号化ライセンス情報を生成する。

【００７０】次いで、ステップＳＴ４０９において、暗号化手段２６０は、ステップＳＴ４０８において得られた暗号化ライセンス情報をメモリカード１００のライセンス記憶手段１３０へ書き込む。通常、メモリカード１００のライセンス記憶手段１３０には、複数のコンテンツの暗号化ライセンス情報が記憶される。そこで、ライセンス記憶手段１３０に暗号化ライセンス情報を書き込む際には、図５に示すように、暗号化ライセンス情報５３に対応づけてコンテンツタイトル５１、コンテンツ付属情報５２なども書き込んでおく。これにより、後で利用者が、複数の暗号化ライセンス情報から希望のコンテンツを指示することが容易となる。

【００７１】このようにして、利用者の希望するコンテンツのライセンス情報が、利用者の携帯するメモリカード１００のライセンス記憶手段１３０に書き込まれる。

【００７２】以上のように、第１の実施形態におけるライセンス発行装置２００は、メモリカード認証手段２１０と、暗号化手段２６０とを設けたため、コンテンツと分離したライセンス情報と、正当と認識されたメモリカード１００へ記憶させることができる。

【００７３】また、利用者が希望するコンテンツ自体は書き込まずにそのコンテンツのライセンス情報だけを、利用者の携帯するメモリカード１００に書き込む。したがって、利用者が希望するコンテンツが大容量のコンテンツであっても、ライセンス情報の発行にかかる時間を増大させることがなく、また、メモリカード１００のライセンス記憶手段１３０の記憶容量を気にする必要もない。

【００７４】また、ライセンス情報のデータ量はコンテンツのデータ量に比べて小さいため、利用者は１つのメ

モリカード１００でたくさんのコンテンツを利用することができる。

【００７５】なお、ここでは、連結手段２５０によって生成されるライセンス情報にはコンテンツ利用条件が含まれているが、コンテンツ利用条件を用いずにコンテンツＩＤとコンテンツ復号化鍵とを連結してライセンス情報を生成してもよい。この場合は、コンテンツ利用条件入力手段２３０を設ける必要はない。

【００７６】また、コンテンツ復号化鍵を用いずにコンテンツＩＤとコンテンツ利用条件とを連結してライセンス情報を生成してもよい。この場合、ライセンス発行装置２００にコンテンツ復号化鍵取得手段２４０を設ける必要はなくなるが、その代わりに、コンテンツ再生装置３００にコンテンツ復号化鍵取得手段を設ける必要がある。

【００７７】＜相互認証の手順＞次に、図４に示したステップＳＴ４０２における相互認証の手順について、図６および図２を参照しつつ説明する。なお、図６中、ステップＳＴ６０１－ＳＴ６０６はメモリカード１００の相手装置認証手段１２０における処理、ステップＳＴ６１１－ＳＴ６１６はライセンス発行装置２００のメモリカード認証手段２１０における処理を示す。

【００７８】認証に先立って、ライセンス発行装置２００のメモリカード認証手段２１０は、メモリカード１００から装置ＩＤ（ｉｄ）を取得する。このように、メモリカード１００およびライセンス発行装置２００は、あらかじめメモリカード１００の装置ＩＤ（ｉｄ）を共有しておく。さらに、メモリカード１００は装置鍵Ｋｄ１を、ライセンス発行装置２００は装置鍵Ｋｄ２を持つ。装置鍵Ｋｄ１，Ｋｄ２は、それぞれの装置自身で保持し、外部から読み出してできないようにしておく。望ましくは、解析できないような耐タンパー装置で防御されている。メモリカード１００およびライセンス発行装置２００がお互いに正当な装置であれば、装置鍵Ｋｄ１と装置鍵Ｋｄ２は同一であるものとする。

【００７９】まず、ステップＳＴ６０１において、メモリカード１００の相手装置認証手段１２０は、暗号化装置ＩＤ（Ｅｉ１）を生成する。暗号化装置ＩＤ（Ｅｉ１）は、メモリカード１００の装置ＩＤ（ｉｄ）を装置鍵Ｋｄ１を用いて暗号化することによって生成される。これを図６では、Ｅｉ１＝Ｆ（Ｋｄ１，ｉｄ）と表している。

【００８０】一方、ステップＳＴ６１１において、ライセンス発行装置２００のメモリカード認証手段２１０は、暗号化装置ＩＤ（Ｅｉ２）を生成する。暗号化装置ＩＤ（Ｅｉ２）は、メモリカード１００の装置ＩＤ（ｉｄ）を装置鍵Ｋｄ２を用いて暗号化することによって生成される。これを図６では、Ｅｉ２＝Ｆ（Ｋｄ２，ｉｄ）と表している。

【００８１】そして以下の処理によって、お互いが有する暗号化装置ＩＤ（Ｅｉ１，Ｅｉ２）が同一であることを、暗号化装置ＩＤ（Ｅｉ１，Ｅｉ２）を装置外部の通信手段を用いてやりとりすることなく確認することによって、お互いの装置の正当性を認証する。

【００８２】ステップＳＴ６０２において、メモリカード１００の相手装置認証手段１２０は、乱数Ｒ１を生成し、ライセンス発行装置２００のメモリカード認証手段２１０へ送信する。

【００８３】そして、ステップＳＴ６０３において、メモリカード１００の相手装置認証手段１２０は、乱数Ｒ１を暗号化装置ＩＤ（Ｅｉ１）を用いて暗号化して暗号化乱数Ｅｒ１を生成する。これを図６では、Ｅｒ１＝Ｅ（Ｅｉ１，Ｒ１）と表している。

【００８４】一方、ステップＳＴ６１２において、ライセンス発行装置２００のメモリカード認証手段２１０は、受信した乱数Ｒ１を暗号化装置ＩＤ（Ｅｉ２）を用いて暗号化して暗号化乱数Ｅ２ｒ１を生成する。これを図６では、Ｅ２ｒ１＝Ｅ（Ｅｉ２，Ｒ１）と表している。そして、ライセンス発行装置２００のメモリカード認証手段２１０は、暗号化乱数Ｅ２ｒ１をメモリカード１００の相手装置認証手段１２０へ送信する。

【００８５】次いで、ステップＳＴ６０４において、メモリカード１００の相手装置認証手段１２０は、ステップＳＴ６０３において生成した暗号化乱数Ｅｒ１と、ステップＳＴ６１２において受信した暗号化乱数Ｅ２ｒ１とを比較する。比較の結果、両者が一致しないときは、ステップＳＴ６０６に進み、相手装置認証手段１２０は、ライセンス発行装置２００が正当なものではないとみなし（エラー発生）、利用者にその旨を知らせる。そして処理を終了する。一方、両者が一致するときは、相手装置認証手段１２０は、ライセンス発行装置２００が正当なものであるとみなし、ステップＳＴ６０５に進む。

【００８６】ステップＳＴ６１３において、ライセンス発行装置２００のメモリカード認証手段２１０は、乱数Ｒ２を生成し、メモリカード１００の相手装置認証手段１２０へ送信する。

【００８７】そして、ステップＳＴ６１４において、ライセンス発行装置２００のメモリカード認証手段２１０は、乱数Ｒ２を暗号化装置ＩＤ（Ｅｉ２）を用いて暗号化して暗号化乱数Ｅ２ｒ２を生成する。これを図６では、Ｅ２ｒ２＝Ｅ（Ｅｉ２，Ｒ２）と表している。

【００８８】一方、ステップＳＴ６０５において、メモリカード１００の相手装置認証手段１２０は、受信した乱数Ｒ２を暗号化装置ＩＤ（Ｅｉ１）を用いて暗号化して暗号化乱数Ｅｒ２を生成する。これを図６では、Ｅｒ２＝Ｅ（Ｅｉ１，Ｒ２）と表している。そして、メモリカード１００の相手装置認証手段１２０は、暗号化乱数Ｅｒ２をライセンス発行装置２００のメモリカード認証手段２１０へ送信する。

【００８９】次いで、ステップＳＴ６１５において、ライセンス発行装置２００のメモリカード認証手段２１０は、ステップＳＴ６１４において生成した暗号化乱数Ｅ２ｒ２と、ステップＳＴ６０５において受信した暗号化乱数Ｅ１ｒ２とを比較する。比較の結果、両者が一致しないときは、ステップＳＴ６１６に進み、ライセンス発行装置２００のメモリカード認証手段２１０は、メモリカード１００が正当なものではないとみなし（エラー発生）、利用者にその旨を知らせる。そして処理を終了する。一方、両者が一致するときは、ライセンス発行装置２００のメモリカード認証手段２１０は、メモリカード１００が正当なものであるとみなす。

【００９０】以上のようにして、メモリカード１００とライセンス発行装置２００との間で、お互いが正当な装置であることの認証（相互認証）が行われる。

【００９１】そして、相互認証の手続きが終了した後、メモリカード認証手段２１０は、暗号化装置ＩＤ（Ｅｉ２）を暗号化手段２６０へ出力する。

【００９２】なお、ここでは装置鍵Ｋｄ１，Ｋｄ２を用いているが、これらを用いず、装置ＩＤに特定の変換Ｆを施してＥｉ１，Ｅｉ２を得ることもできる。この場合は、変換Ｆを非公開にして、変換方法が共通である装置を正当な装置を認証することとなる。

【００９３】<コンテンツ再生装置３００の構成>図７は、図１に示したメモリカード１００およびコンテンツ再生装置３００の具体的な構成を示すブロック図である。以下、図７を参照してコンテンツ再生装置３００の具体的な構成について説明する。

【００９４】コンテンツ再生装置３００は、メモリカード認証手段２１０と、コンテンツＩＤ入力手段２２０と、復号手段３１０と、分離手段３２０と、比較手段３３０と、再生手段３４０と、暗号化コンテンツデータベース３５０とを備える。

【００９５】復号手段３１０は、メモリカード１００のライセンス記憶手段１３０に記憶された暗号化ライセンス情報を読み出し、読み出した暗号化ライセンス情報をメモリカード認証手段２１０からの暗号化装置ＩＤを用いて復号してライセンス情報を得る。

【００９６】分離手段３２０は、復号手段３１０によって得られたライセンス情報から、コンテンツＩＤ、コンテンツ利用条件、およびコンテンツ復号化鍵を得る。

【００９７】比較手段３３０は、分離手段によって得られたコンテンツＩＤとコンテンツＩＤ入力手段２２０によって得られたコンテンツＩＤとを比較し、両者が一致するときは、再生指示信号を再生手段３４０に出力する。

【００９８】暗号化コンテンツデータベース３５０には、コンテンツをそのままでは利用ができないように暗号化した暗号化コンテンツが格納されている。

【００９９】再生手段３４０は、比較手段３３０からの再生指示信号に応答して、分離手段３２０によって得られたコンテンツＩＤに対応する暗号化コンテンツを暗号化コンテンツデータベース３５０から取得する。そして再生手段３４０は、取得した暗号化コンテンツを分離手段３２０によって得られたコンテンツ復号化鍵を用いて復号し、分離手段３２０によって得られたコンテンツ利用条件に従って再生する。

【０１００】<コンテンツの再生の手順>図８は、図７に示したコンテンツ再生装置３００によるコンテンツの再生の手順を示すフローチャートである。以下、図８および図７を参照しつつコンテンツの再生の手順について説明する。

【０１０１】まず、ステップＳＴ８０１において、利用者は、再生を希望するコンテンツに対する暗号化ライセンス情報が記憶されたメモリカード１００をコンテンツ再生装置３００の所定の挿入口に差し込む。これにより、メモリカード１００に設けられたピンとコンテンツ再生装置３００のソケットとの間が電気的に接続される。この結果、メモリカード１００とコンテンツ再生装置３００との間で、お互いにデータを送受信するための通信手段が確保される。

【０１０２】次いで、ステップＳＴ８０２において、メモリカード１００とコンテンツ再生装置３００との間で、お互いが正当な装置であることの認証が行われる。この相互認証は、図６に示したのと同様の手順で行われる。相互認証を行った後、コンテンツ再生装置３００のメモリカード認証手段２１０は、メモリカード１００の装置ＩＤを暗号化して暗号化装置ＩＤを生成する。

【０１０３】次いで、ステップＳＴ８０３において、利用者は、コンテンツＩＤ入力手段２２０を利用して、再生を希望するコンテンツに対するコンテンツＩＤを入力する。通常、メモリカード１００のライセンス記憶手段１３０には、複数の暗号化ライセンス情報が記憶されている。しかし、図５に示したように、メモリカード１００のライセンス記憶手段１３０には、暗号化ライセンス情報５３に対応づけてコンテンツタイトル５１、コンテンツ付属情報５２なども記憶されている。したがって、メモリカード１００のライセンス記憶手段１３０に記憶されているコンテンツタイトル／コンテンツ付属情報の一覧を利用者に提示して、希望するコンテンツタイトルを選択させた後、図３に示したのと同様のデータベースを用いてコンテンツＩＤを得ることができる。

【０１０４】次いで、ステップＳＴ８０４において、復号手段３１０は、メモリカード１００のライセンス記憶手段１３０から、利用者が再生を希望するコンテンツに対する暗号化ライセンス情報を読み出す。ここでは、ステップＳＴ８０３において利用者が選択したコンテンツタイトルを用いることによって、復号すべき暗号化ライセンス情報を容易に特定することができる。そして、復号手段３１０は、読み出した暗号化ライセンス情報を、

ステップＳＴ８０２においてメモリカード認証手段２１０によって生成された暗号化装置ＩＤを用いて復号し、ライセンス情報を得る。

【０１０５】次いで、ステップＳＴ８０５において、分離手段３３０は、復号手段３１０によって得られたライセンス情報を、コンテンツＩＤ、コンテンツ復号化鍵、およびコンテンツ利用条件に分離する。

【０１０６】次いで、ステップＳＴ８０６において、比較手段３３０は、ステップＳＴ８０３においてコンテンツＩＤ入力手段２２０によって得られたコンテンツＩＤと、ステップＳＴ８０５において分離手段３２０によって得られたコンテンツＩＤとを比較する。比較の結果、両者が同一であれば、このライセンス情報は正当なライセンス発行装置によって発行されたものであるとみなし、比較手段３３０は、再生指示信号を再生手段３４０に出力する。

【０１０７】次いで、ステップＳＴ８０７において、再生手段３４０は、比較手段３３０からの再生指示信号に応答して、分離手段３２０によって得られたコンテンツＩＤに対応する暗号化コンテンツを暗号化コンテンツデータベース３５０から取得する。そして再生手段３４０は、取得した暗号化コンテンツを分離手段３２０によって得られたコンテンツ復号化鍵を用いて復号し、分離手段３２０によって得られたコンテンツ利用条件に従って再生する。例えば、コンテンツ利用条件として利用可能な期限が付加されたものであれば、現在の日付と利用可能な期限とを比較することにより、再生を行うかどうかを再生前に判断する。

【０１０８】このようにして、利用者が希望するコンテンツの再生が行われる。

【０１０９】以上のように、第１の実施形態におけるコンテンツ再生装置３００は、メモリカード認証手段２１０と、復号手段３１０と、再生手段３４０とを設けたため、コンテンツと分離したライセンス情報を、正当と認識されたメモリカード１００から読み込んで、対応するコンテンツを再生することができる。

【０１１０】なお、ここでは、暗号化コンテンツデータベース３５０をコンテンツ再生装置３００内に設けたが、これを外部、例えば、通信回線を介して遠隔地に設けてもよい。この場合、コンテンツ再生装置３００は、コンテンツＩＤのような情報でコンテンツを特定して、外部にある暗号化コンテンツデータベースより暗号化コンテンツを受信し、再生する。このように暗号化コンテンツデータベースを外部に設けることは、コンテンツ再生装置が大きな記憶容量を確保できない携帯端末である場合に有利である。

【０１１１】また、メモリカード１００のライセンス記憶手段１３０に記憶されたライセンス情報にコンテンツ利用条件が含まれていない場合には、分離手段３２０ではコンテンツ利用条件は得られない。したがって、コンテンツ再生手段３４０は利用条件を考慮する必要はない。

【０１１２】また、メモリカード１００のライセンス記憶手段１３０に記憶されたライセンス情報にコンテンツ復号化鍵が含まれていない場合には、図５に示したようなコンテンツＩＤとコンテンツ復号化鍵とを対応づけたデータベースを設けておき、このデータベースを用いて、分離手段３２０によって得られたコンテンツＩＤよりコンテンツ復号化鍵を得ることができる。

【０１１３】また、メモリカード１００のライセンス記憶手段１３０から読み込んだ暗号化ライセンス情報が十分信頼できるものである場合には、コンテンツＩＤ入力手段２２０および比較手段３３０を取り除いた構成とすることも可能である。

【０１１４】また、図２に示したライセンス発行装置２００の暗号化手段２６０および図７に示したコンテンツ再生装置３００の復号化手段３１０では、暗号／復号の鍵としてメモリカード認証手段２１０からの暗号化装置ＩＤを用いているが、これに代えて、外部から読み出し不可能な非公開の鍵をライセンス発行装置２００およびコンテンツ再生装置３００にあらかじめ記憶させておき、これを暗号／復号の鍵としてもよい。さらにこの場合、暗号化／復号化の暗号アルゴリズムとして、例えばＲＳＡのような非対称暗号を用い、それぞれの装置で対応する鍵を記憶しておくこともできる。

【０１１５】<効果>以上のように、この発明の第１の実施形態によるコンテンツ提供システムでは、ライセンス発行装置２００は、コンテンツのライセンス情報を、携帯可能な独立したハードウエアであるメモリカード１００に書き込む。そして、コンテンツ再生装置３００は、メモリカード１００に記憶されたライセンス情報に従ってコンテンツを再生する。したがって、利用者は、希望するコンテンツのライセンス情報が書き込まれたメモリカード１００を携帯し、ライセンス発行装置２００に対応したさまざまな形態のコンテンツ再生装置３００を利用してコンテンツの提供を受けることができる。すなわち、利用者は、コンテンツ再生装置３００の形態に制限されることなく、購入したコンテンツを利用することができる。

【０１１６】また、ライセンス情報は、暗号化装置ＩＤを用いて暗号化／復号化される。すなわち、ライセンス情報は、個々のメモリカード１００を一意に識別可能な装置ＩＤを用いて暗号化／復号化される。これにより、暗号化ライセンス情報を不正にコピーしたメモリカードを用いてコンテンツの提供を受けるような不正な利用を防ぐことができる。

【０１１７】また、ライセンス発行装置２００はコンテンツのライセンス情報だけを、利用者の携帯するメモリカード１００に書き込む。したがって、利用者が希望するコンテンツが大容量のコンテンツであっても、ライセ

ンス情報の発行にかかる時間を増大させることがなく、また、メモリカード１００のライセンス記憶手段１３０の記憶容量を気にする必要もない。

【００１８】また、ライセンス情報のデータ量はコンテンツのデータ量に比べて小さいため、利用者は１つのメモリカード１００でたくさんのコンテンツを利用することができる。

【００１９】また、コンテンツは暗号化されて配布され、ライセンス情報を購入しなければ再生が不可能なため、ネットワーク、放送、パッケージなど形態を問わず自由に流通させることが可能となり、かつ、利用者にとっては入手が容易となる。これにより、利用者は必ずしもコンテンツを所有する必要がなく、ライセンス情報のみを購入、携帯し、必要に応じてコンテンツにアクセスすればよい。この結果、利用者側でコンテンツを蓄積するための大容量のデータ蓄積装置を確保できない場合は、コンテンツの再生時にその都度ダウンロードすることによって、仮想的に容量が無限大のコンテンツサーバを所有することと同様の効果が得られる。一方、利用者側に大容量のデータ蓄積装置を確保できる場合は、事前に再生する可能性のあるコンテンツをすべてダウンロードしておき、再生時にはライセンス情報を購入することによって、ダウンロードに時間のかかる大容量のコンテンツを即座に再生することが可能となる。

【００２０】（第２の実施形態）この発明の第２の実施形態によるコンテンツ提供システムでは、図７に示したコンテンツ再生システム３００に代えて、図９に示すコンテンツ再生装置９００を備える。そして、その他の構成を第１の実施形態におけるコンテンツ提供システムと同じくする。

【００２１】＜コンテンツ再生装置９００の構成＞図９を参照して、このコンテンツ再生装置９００は、メモリカード認証手段２１０と、コンテンツＩＤ入力手段２２０と、復号手段３１０と、分離手段３２０と、比較手段３３０と、再生手段３４０と、暗号化コンテンツデータベース３５０と、コンテンツ利用条件更新手段９１０と、連結手段９２０と、暗号化手段９３０と、暗号化ライセンス情報更新手段９４０とを備える。

【００２２】再生手段３４０は、第１の実施形態において説明した動作に加えてさらに、コンテンツを再生したことを示す再生検知信号を生成し、コンテンツ利用条件を出力する。

【００２３】コンテンツ利用条件更新手段９１０は、コンテンツ再生手段３４０からの再生検知信号を受けて、コンテンツ再生手段３４０からコンテンツ利用条件を読み込み、当該コンテンツ利用条件を更新して更新後コンテンツ利用条件を生成する。これは、コンテンツの再生前後でコンテンツ利用条件が変化する場合（例えば、コンテンツ利用条件として「コンテンツを利用することができる回数」が定められている場合など）を想定している。このように利用回数に制限が存在する場合は、１回再生するごとに残りの利用回数を減じていかなければならない。そして減じた後の利用回数を新たにコンテンツの利用条件として更新することが必要となる。

【００２４】連結手段９２０は、コンテンツ利用条件更新手段９１０からの更新後コンテンツ利用条件と、分離手段３２０からのコンテンツＩＤおよびコンテンツ復号化鍵とを連結して、更新後ライセンス情報を生成する。

【００２５】暗号化手段９３０は、連結手段９２０からの更新後ライセンス情報をメモリカード認証手段２１０からの暗号化装置ＩＤを用いて暗号化して、更新後暗号化ライセンス情報を生成する。

【００２６】暗号化ライセンス情報更新手段９４０は、メモリカード１００のライセンス記憶手段１３０に記憶されている暗号化ライセンス情報を、暗号化手段９３０によって生成された更新後暗号化ライセンス情報に書き換える。

【００２７】＜コンテンツ再生装置９００の動作＞以下、図９に示したコンテンツ再生装置９００の動作について説明する。

【００２８】コンテンツ再生装置９００は、図８に示したステップＳＴ８０１－ＳＴ８０７における処理と同様の処理によってコンテンツの再生を行う。

【００２９】そして、コンテンツの再生が終了した後またはコンテンツの再生中に、再生手段３４０は、再生検知信号をコンテンツ利用条件更新手段９１０に出力する。

【００３０】次いで、コンテンツ利用条件更新手段９１０は、再生検知信号を受けて、再生手段３４０からコンテンツ利用条件を読み込み、当該コンテンツ利用条件のうち再生に応じて変更すべき部分を変更する。例えば、コンテンツ利用条件が「再生可能な回数は３である」という条件であれば、再生可能な回数を１減じて２と変更する。そして、これを更新後コンテンツ利用条件として連結手段９２０へ出力する。

【００３１】次いで、連結手段９２０は、更新後コンテンツ利用条件と、コンテンツＩＤと、コンテンツ復号化鍵とを連結して、更新後ライセンス情報を生成する。

【００３２】次いで、暗号化手段９３０は、更新後ライセンス情報を暗号化装置ＩＤを用いて暗号化する。

【００３３】次いで、暗号化ライセンス情報更新手段９４０は、メモリカード１００のライセンス記憶手段１３０に記憶されている暗号化ライセンス情報を消去し、更新後暗号化ライセンス情報を書き込む。

【００３４】＜効果＞以上のように、第２の実施形態によるコンテンツ再生装置９００は、コンテンツ利用条件更新手段９１０と、連結手段９２０と、暗号化手段９３０と、暗号化ライセンス情報更新手段９４０とを設けたため、コンテンツの再生に応じてコンテンツ利用条件が変化する場合でも、コンテンツ利用条件を更新すること

ができ、正しいコンテンツ利用条件を保持することが可能となる。

【０１３５】（第３の実施形態）図１０は、図１に示したコンテンツ提供システムの適用例を示す図である。以下、図１０を参照して、コンテンツ提供システムの適用例について説明する。

【０１３６】ライセンス発行装置２００は、駅、コンビニ、店頭などに設置されたり（２００ａ）、パソコンや携帯電話などの端末４００から有線、無線を問わずアクセス可能なネットワークに接続されたりする（２００ｂ）。そして、利用者は、ライセンス発行装置２００ａまたは端末４００にメモリカード１００を挿入し、ガイダンスに従って希望のコンテンツ（音楽、映画、ゲーム、電子本など）を選択して、表示された料金を支払う。ライセンス発行装置２００ａ，２００ｂは、利用者が選択したコンテンツに対するライセンス情報を、メモリカード１００の装置ＩＤを用いて暗号化してメモリカード１００へ書き込む。書き込みが終了すると、利用者はレシートを受け取り、メモリカード１００を取り出す。このように、利用者は、自宅／外出先のいずれにおいても、希望するコンテンツの暗号化ライセンス情報をメモリカード１００に書き込むことができる。そして、利用者は、ＣＤやＭＤなどの希望のコンテンツが格納された媒体を持ち歩く必要はなく、ライセンス情報だけが書き込まれたメモリカード１００を携帯すればよい。

【０１３７】一方、コンテンツは、そのままでは利用ができないように暗号化して暗号化コンテンツとして、ネットワーク、放送、パッケージなどのさまざまな形態で流通している。

【０１３８】そして、利用者の自宅に設けられたホームサーバ３５０ａには、パソコンからネットワーク経由でダウンロードした暗号化コンテンツや、デジタルＴＶのデータ放送を受信して得られた暗号化コンテンツなどが蓄積されている。利用者は、希望するコンテンツの暗号化ライセンス情報が書き込まれたメモリカードを自宅にあるコンテンツ再生装置３００ａに挿入することによって、コンテンツの提供を受けることができる。

【０１３９】また、外出先（列車、飛行機などの交通機関、自動車、店、図書館、ホテルなど）にも、コンテンツサーバ３５０ｂ、コンテンツ再生装置３００ｂが設けられている。コンテンツ再生装置３００ｂは、コンテンツの提供者側が用意するものであってもよいし、利用者が所持する携帯端末を利用してもよい。利用者は、希望するコンテンツの暗号化ライセンス情報が書き込まれたメモリカードをコンテンツ再生装置３００ｂに挿入することによって、コンテンツの提供を受けることができる。

【０１４０】コンテンツ提供者にとっては、豊富なコンテンツを提供することによる集客効果、差別化、徴収した利用料などのメリットが得られる。また、コンテンツの再生中にＣＭを流して広告収入を得たり、自店舗の紹介をしたりすることができる。さらに、高音質、高画質を売りにしたコンテンツ再生装置を用意して、その利用料を徴収することもできる（例えば、ハイビジョン映像なら１００円増しにするなど）。

【０１４１】利用者にとっては、好きな音楽を、自宅、車の中、電車の中、船の中、飛行機の中などで聴くことができる。しかも、ＣＤやＭＤなどの媒体や再生装置を持ち歩く必要がなく、メモリカード１枚だけでよい。

【０１４２】また、利用者は、最近はやりの個室スペースで、音楽を聴いたり、映画を見たり、本を読んだり、ゲームをしたりというようにさまざまなコンテンツを提供を受けることができる。この場合、個室スペースの提供者は、メモリカードにライセンス情報が書き込まれていれば個室スペースの利用料を無料とすることもできる。ライセンス発行装置が設けられていれば、利用者は、メモリカードにライセンス情報が書き込まれていない場合にも、その場で購入することができる。

【０１４３】また、利用者は、旅行先で見所を調べるために、旅行前に買った雑誌（コンテンツ）へアクセスして調べることもできる。これにより、利用者は、雑誌、新聞、百科事典などを持ち歩く必要がなくなる。

【０１４４】

【発明の効果】この発明の１つの局面に従ったライセンス発行装置は、利用者が希望するコンテンツのライセンス情報を、携帯可能な独立したハードウエアであるライセンス記憶装置に書き込む。したがって、利用者は、希望するコンテンツのライセンス情報が書き込まれたライセンス記憶装置を携帯し、ライセンス記憶装置に対応したさまざまな形態のコンテンツ再生装置を利用してコンテンツの提供を受けることができる。

【０１４５】また、ライセンス情報は、ライセンス記憶装置の装置ＩＤを用いて暗号化されるため、暗号化ライセンス情報を不正にコピーしたライセンス記憶装置を用いてコンテンツの提供を受けるような不正な利用を防ぐことができる。

【０１４６】また、コンテンツのライセンス情報だけを利用者の携帯するライセンス記憶装置に書き込むため、利用者が希望するコンテンツが大容量のコンテンツであっても、ライセンス情報の発行にかかる時間を増大させることがなく、また、利用者はライセンス記憶装置の記憶容量を気にする必要もない。

【０１４７】また、ライセンス情報のデータ量はコンテンツのデータ量に比べて小さいため、利用者は１つのライセンス記憶装置でたくさんのコンテンツを利用することができる。

【０１４８】また、ライセンス発行装置は、利用者が携帯するライセンス記憶装置にネットワークを介して接続されるため、利用者はライセンス発行装置と距離的に離れた所にいても、ネットワークを介してライセンス発行

装置にアクセス可能な携帯端末などを用いて、ライセンス情報の発行を受けることができる。

【0149】この発明のもう1つの局面に従ったコンテンツ再生装置は、利用者が携帯するライセンス記憶装置に書き込まれたライセンス情報を用いて暗号化コンテンツを復号し再生する。したがって、利用者は、希望するコンテンツのライセンス情報が書き込まれたライセンス記憶装置を携帯し、ライセンス記憶装置に対応したさまざまな形態のコンテンツ再生装置を利用してコンテンツの提供を受けることができる。

【0150】また、利用者が携帯するライセンス記憶装置に書き込まれたライセンス情報は、当該ライセンス記憶装置の装置IDを用いて復号されるため、暗号化ライセンス情報を不正にコピーしたライセンス記憶装置を用いてコンテンツの提供を受けるような不正な利用を防ぐことができる。

【0151】また、蓄積手段を設けたため、再生する可能性のあるコンテンツをあらかじめすべて蓄積しておくことができる。これにより、取得するのに時間のかかる大容量のコンテンツであっても即座に再生することができる。

【0152】また、再生手段は、復号手段によって得られたライセンス情報において利用を許可されているコンテンツに対応する暗号化されたコンテンツをネットワークを介して取得するため、コンテンツの再生時にその都度暗号化コンテンツをネットワークを介して取得することができる。これにより、仮想的に容量が無限大のコンテンツサーバを所有することと同様の効果が得られる。

【0153】また、コンテンツ利用条件更新手段と、更新後ライセンス情報生成手段と、暗号化手段と、書き換え手段とを設けたため、コンテンツの再生に応じてコンテンツ利用条件が変化する場合でも、コンテンツ利用条件を更新することができ、正しいコンテンツ利用条件を保持することができる。

【0154】この発明のさらにもう1つの局面に従ったライセンス発行方法は、利用者が希望するコンテンツのライセンス情報を、携帯可能な独立したハードウエアであるライセンス記憶装置に書き込む。したがって、利用者は、希望するコンテンツのライセンス情報が書き込まれたライセンス記憶装置を携帯し、さまざまな形態のコンテンツ再生装置を利用してコンテンツの提供を受けることができる。

【0155】この発明のさらにもう1つの局面に従ったコンテンツ再生方法は、利用者が携帯するライセンス記憶装置に書き込まれたライセンス情報を用いて暗号化コンテンツを復号し再生する。したがって、利用者は、希望するコンテンツのライセンス情報が書き込まれたライセンス記憶装置を携帯し、さまざまな形態のコンテンツの提供を受けることができる。

【図面の簡単な説明】

【図1】この発明の第1の実施形態によるコンテンツ提供システムの構成を示す図である。

【図2】図1に示したメモリカードおよびライセンス発行装置の具体的な構成を示すブロック図である。

【図3】コンテンツタイトル、コンテンツID、およびコンテンツ復号化鍵が対応づけられたデータベースのデータ構造を示す図である。

【図4】図2に示したライセンス発行装置によるライセンス情報の発行の手順を示すフローチャートである。

【図5】メモリカードのライセンス記憶手段に記憶される情報を示す図である。

【図6】メモリカードとライセンス発行装置との間での相互認証の手順を示すフローチャートである。

【図7】図1に示したメモリカードおよびコンテンツ再生装置の具体的な構成を示すブロック図である。

【図8】図7に示したコンテンツ再生装置によるコンテンツの再生の手順を示すフローチャートである。

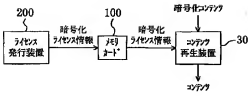
【図9】この発明の第2の実施形態によるコンテンツ再生装置の構成を示すブロック図である。

【図10】図1に示したコンテンツ提供システムの適用例を示す図である。

【符号の説明】

100 メモリカード
120 相手装置認証手段
130 ライセンス記憶手段
200, 200a, 200b ライセンス発行装置
210 メモリカード認証手段
250, 920 連結手段
260, 930 暗号化手段
300, 900, 300a, 300b コンテンツ再生装置
310 復号手段
340 再生手段
350, 350a, 350b 暗号化コンテンツデータベース
910 コンテンツ利用条件更新手段
940 暗号化ライセンス情報更新手段

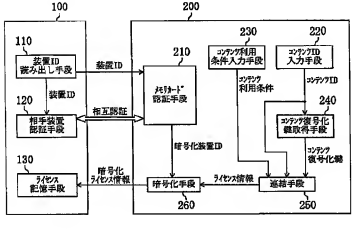
【図1】



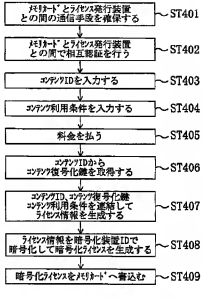
【図3】

31	32	33
音楽1	0001	SSSS1
音楽2	0002	TTTT2
映画1	0003	UUUU3
映画2	0004	VVVV4
:	:	:

【図2】



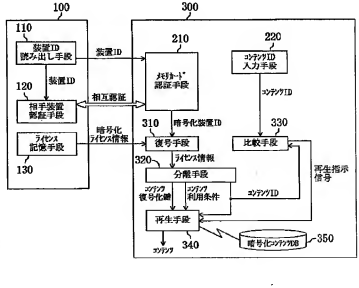
【図4】



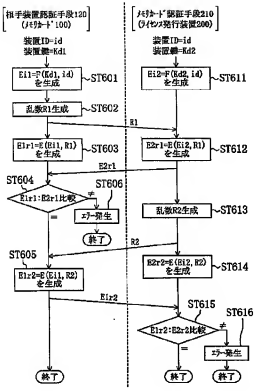
【図5】

51	52	53
音楽A	歌手1	XXABCD
音楽B	歌手2	XXEFGH
映画A	俳優1	XXIJKLM
:	:	:

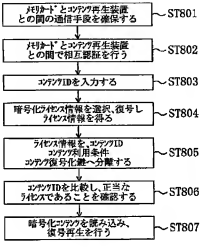
【図7】



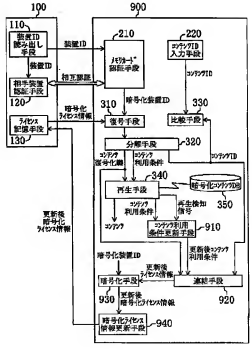
【図6】


相手装置認証手段120
(メモリカード100)
装置ID=id
装置鍵=Kd1
E11=E(Kd1, Id)
を生成
ST601
乱数R1生成
ST602
R1
E1r1=E(E11, R1)
を生成
ST603
E2r1
ST604
E1r1:E2r1比較
ST606
エラー発生
終了
R2
ST605
E1r2=E(E11, R2)
を生成
E1r2
終了
メモリカード認証手段210
(ライセンス発行装置200)
装置ID=id
装置鍵=Kd2
E12=E(Kd2, Id)
を生成
ST611
E2r1=E(E12, R1)
を生成
ST612
乱数R2生成
ST613
E2r2=E(E12, R2)
を生成
ST614
ST615
E1r2:E2r2比較
ST616
エラー発生
終了
終了

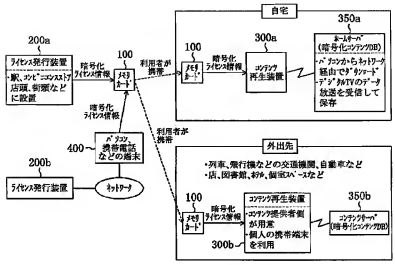
【図8】


メモリカードとコンテンツ再生装置
との間の通信手段を確保する
ST801
メモリカードとコンテンツ再生装置
との間で相互認証を行う
ST802
コンテンツIDを入力する
ST803
暗号化ライセンス情報を選択、復号し
ライセンス情報を得る
ST804
ライセンス情報を、コンテンツID
コンテンツ利用条件、
コンテンツ復号化鍵へ分離する
ST805
コンテンツIDを比較し、正当な
ライセンスであることを確認する
ST806
暗号化コンテンツを読み込み、
復号再生を行う
ST807

【図9】


100
900
110
記憶ID
読み出し
手段
装置ID
相手装置
認証手段
120
ライセンス
記憶手段
130
210
装置ID
メモリカード
認証手段
特定鍵
220
コンテンツID
入力手段
コンテンツID
暗号化装置ID
310
330
暗号化
ライセンス情報
復号手段
比較手段
分離手段
320
コンテンツ
復号化鍵
コンテンツ
利用条件
コンテンツID
340
暗号化コンテンツ格納
再生手段
コンテンツ
利用条件
再生検知
信号
350
コンテンツ
コンテンツ利用
条件更新手段
910
更新後
暗号化
ライセンス情報
更新後コンテンツ
利用条件
暗号化装置ID
更新後
ライセンス情報
暗号化手段
連結手段
930
更新後
暗号化ライセンス情報
920
暗号化ライセンス
格納更新手段
940

【図10】



フロントページの続き

(51)Int.Cl.⁷	識別記号	FI		テーマコード(参考)
G06F 17/60	302	G06F	9/06	660F
H04L 9/08		H04L	9/00	601A
9/32				673B